(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 February 2004 (12.02.2004)

PCT

(10) International Publication Number
WO 2004/014045 A1

(51) International Patent Classification[7]: H04L 29/12, 29/06, 12/14

(21) International Application Number: PCT/EP2003/007544

(22) International Filing Date: 11 July 2003 (11.07.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
02016542.9 24 July 2002 (24.07.2002) EP

(71) Applicant *(for all designated States except US)*: INTERNATIONAL BUSINESS MACHINES CORPORATION [US/US]; New Orchard Road, Armonk, NY 10504 (US).

(71) Applicant *(for LU only)*: IBM DEUTSCHLAND GMBH [DE/DE]; Pascalstrasse 100, 70569 Stuttgart (DE).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: KRAEMER, Ulrich [DE/DE]; Frankfurter Strasse 76, 64293 Darmstadt (DE). LENTZ, Thomas [DE/DE]; Homburgerstr. 10, 60486 Frankfurt/M (DE). WERNER, Andreas [DE/DE]; Am Pfingstborn 10, 61479 Glashuetten (DE).

(74) Agent: KAUFFMANN, Wolfgang; IBM Deutschland GmbH, Intellectual Property, 70548 Stuttgart (DE).

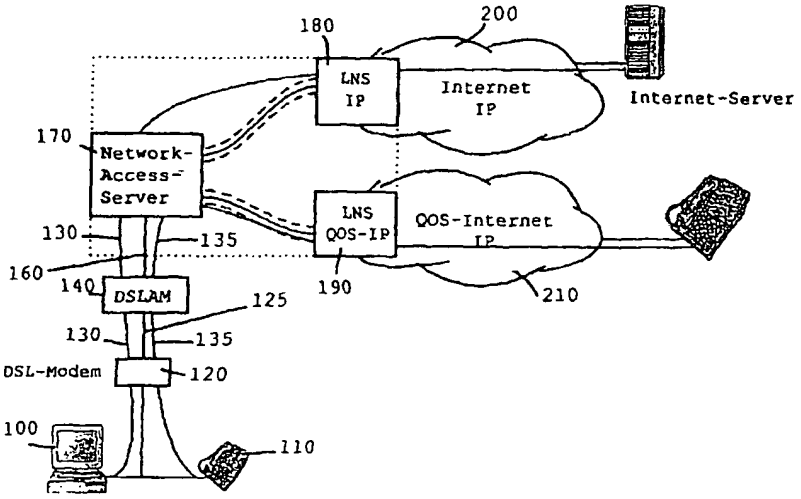
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: SERVICE CLASS DEPENDANT ASIGNMENT OF IP ADDRESSES FOR COTROLLING ACCESS TO AN D DELIVERY OF E-SEVICES



(57) Abstract: For controlling access to and delivery of electronic services in an Internet Protocol (IP) based network environment, services requiring distinct sets of service parameters (QoS levels, filters) are separated by assigning certain quantities of IP addresses to different services or classes of services. If assigned statically, a certain IP address is assigned to a certain application, user or hardware device. Thus, depending on a requested service comprising a certain service attribute or set of service attributes like QoS level (s), a particular - the requested service enabling - IP address is assigned or granted, e.g. from a pool of available IP addresses.The proposed mechanism thus grants or denies access to a requested service or service infrastructure based on a currently assigned IP address and guarantees that all data packets are transferred in a particular way and/or via a particular network infrastructure.

WO 2004/014045 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SERVICE CLASS DEPENDENT ASIGNMENT OF IP ADDRESSES FOR CONTROLLING ACCESS TO AND DELIVERY OF E-SERVICES

BACKGROUND OF THE INVENTION

The invention generally relates to the arena of handling electronic services on an Internet Protocol (IP) based digital network and more specifically to a method and system for controlling access to and delivery of electronic services in such a network environment.

Nowadays there are known many Business-to-Customer (B2C) or Business-to-Business (B2B) services being provided or delivered electronically by Internet Service Providers (ISPs) that require at least a certain quality-of-service (QoS) level for the delivery to a service recipient. Only exemplarily it is referred to electronic services like media streaming (video-on-demand, audio-on-demand, etc.), IP based telephony i.e. Voice-over-IP (VoIP), multi-user support of computer games where a number of users are playing games interactively via a computer network. Thus professional websites or web portals offering or providing the aforementioned services need to have implemented a process for limiting user access to those users having necessary access rights.

A known objective in that business arena thus is user authentication vis-à-vis an ISP. As the Internet Protocol, under a process view, is stateless, in order to guarantee authenticity of a user entering an access restricted website

or web portal, it is necessary to perform a user authentication procedure every time when entering a website or web portal.

Thereupon, accounting or billing of a delivered service within the Internet is not solved at the moment in general. Nowadays every ISP has to use an own application specific solution.

A known approach simplifying the aforementioned user authentication or identification process is disclosed in non-published European Patent Application 01130600.8, which is enclosed herein entirely by reference. Disclosed therein is a managing or server instance preferably implemented as a middleware arranged between an IP layer and a server layer within the well-known Open Systems Interconnection (OSI) reference model that allows for a one time and unique user or subscriber logon (single sign-on). The server instance provides a pool of IP addresses available for allocation to such users. With the approval of a user logon, the server instance allocates an IP address from the pool and a network access server (NAS) establishes a continuous point-to-point (PPP) IP (tunneling) connection between the IP network and the user's computer or telecommunication device. At the same time, the user's IP address together with any attributes relevant for accounting, authentication and authorization (AAA) are recorded or stored. Furthermore, the user's network access is continuously monitored and it is determined if said online session is terminated. If so, the allocated IP address for the user is invalidated and said IP address provided back to said pool of IP addresses.

The mechanism disclosed in the above referenced European patent application thus securely prevents abuse or misuse of

an already assigned IP address for receiving or consuming an above mentioned electronic service. Reliability of that mechanism is mainly obtained through the combination of the continuous IP connection and the direct monitoring of the user's network access behavior. In addition, the user's current IP address is used as an authorization token during the following online session. Now, the stored information can be made available by the server instance to an e-Company where the particular user/subscriber has a valid subscription, standard protocols to IP applications for authentication, authorization, and accounting can be applied between the e-Company and any e-service provider with whom the user/subscriber is interested to conduct any kind of e-Commerce business.

In a B2C scenario, that mechanism therefore allows a user to approach different commercial websites or portals on the Internet during a continuously maintained online session in order to perform different B2C transactions as mentioned above. For handling those transactions, the user is not required to conduct further sign-on procedures on side of the e-service providers again and again since the server instance keeps an existing measure for authenticity of the user. Further, AAA procedures are handled by only one instance, namely the server instance according to the invention. The invention hence is a general solution to the problem of reliable Authentication, Authorization, and Accounting regardless of the technology and method to access the IP services.

It is noteworthy that the above mentioned abuse or misuse is effectively prevented by means of a session context that comprises or includes transaction events performed by the

user, in particular accounting starts or the like in order to continuously keep valid authenticity of the user during a whole online session and in order to use the existing authorization by the user end-to-end business transactions like video-on-demand services offered on websites or Internet portals of e-service providers respectively e-companies.

The above approach, in addition, enables to securely manage the above-mentioned services, despite the pre-mentioned statelessness of TCP/IP protocol, and thus effectively prevents the sales-entity and/or service provider from intrusions by others, i.e. non-authorized accesses to access-restricted websites or Internet portals, due to the session context related access control based on the unique IP address. The randomly changing IP address between successive sessions guarantees maximum secure access authorization handling and thus efficiently protects sales-entity and/or service providers against illegal intrusions by unauthorized users but with minimum-security efforts. It is further to be noted that the session context, due to its randomized character and its location on the middleware provider's premises, can not be simulated or manipulated by an intruder.

Another IP packet based service with high QoS requirements in respect of the necessary speech quality is the known IP packet telephony (IPT), often called "Voice-over-IP" (VoIP). VoIP is voice delivered using the Internet Protocol (IP) and a set of facilities for managing the delivery of voice information using the IP. In general, this means sending voice information in digital form in discrete packets rather than in the traditional circuit-committed protocols of the public switched telephone network (PSTN). It should be mentioned that PSTN concerning circuit switched voice systems includes but is not

limited to plain old telephone systems (POTS) and the known integrated services digital network (ISDN). VoIP uses a real-time protocol (RTP/RTSP) to help ensure that packets get delivered in a timely way. Using public networks, it is currently difficult to guarantee QoS. Better service is possible with private networks managed by an Enterprise or by an Internet telephony service provider (ITSP).

Concerning IP packet telephony (IPT), it is further referred to a relating White Paper by Cisco Systems, Inc. describing the future direction of IPT. The White Paper is e.g. available under the Internet address www.pluscom.ru/general/library/VoIP/ptsguide.pdf. The IPT scenario disclosed therein is based on a distributed, standards-based, packet switching infrastructure, which is independent of the call control and application. This enables provision of transport telephony services over an IP, ATM, or Frame Relay packet/cell infrastructure with the same call control and quality of service (QoS) across the network.

In addition, it is referred to an IPT solution by Ericsson for merging voice, data, and multimedia communications onto one integrated network delivering packet technology over all networks. That solution further provides multiple IP network support and allows QoS control capability and high-quality service availability while minimizing IP transport costs over a variety of IP networks. Accounting is based on the known Remote Authentication Dial-In User Service (RADIUS) protocol explained in more detail afterwards using an Authentication, Authorization and Accounting (AAA) server which enables provision IP telephony central call detail record (CDR) information. The real-time billing includes fraud prevention and, in addition, enables a call duration advice to the

caller; supports third party billing systems.

In known IP packet or network usage based billing of IP services scenarios, a caller client module initiates a call to a receiver using its IP address. The client module invokes a data collector that captures voice packets sent to the receiver. A client billing module hereby counts the number of transmitted packets. When the call is finished, the client module sends the number of packets to a server module. The server module registers the data of the call inside a billing database. The server module then calculates the costs of the call based on a certain rating policy and then sends it to the calling client. On receiving the costs, the client module pops up a window showing information on the call like the costs, the duration and the amount of traffic transferred.

It should be mentioned that a VoIP call performed between a user's personal computer and a POT has to be transferred via the Internet (IP based) at first to a PSTN gateway for translating the transferred IP packets into circuit switched voice and the receiver's telephone number and then transmitted via a PSTN to the telephone device of the receiver of the call.

Another approach for billing a VoIP call is disclosed in published US Patent application ser. No. 20010047333 A1. The mechanism for billing of IP data usage disclosed therein starts with billing a call at a time point where the called party answers the call. An extension subscriber connection processor of a calling party's VoIP gateway determines whether the called party responds to the call from the calling party, and upon receipt of the response, informs a VoIP trunk connection processor of receipt of the response. The VoIP

trunk connection processor receives the response information from the called party at the extension subscriber connection processor, assembles a response packet, and transmits the assembled response packet to the calling party's VoIP gateway through a VoIP call channel. The calling party's VoIP gateway checks the response packet out of the packets received through the call channel, and transmits the checked response packet to a VoIP call processing central controller. The VoIP call processing central controller records a call start time for the corresponding VoIP call using the response information received from the VoIP trunk connection processor.

It should be mentioned that it is not clear for what to bill for a VoIP call since costs are generated by the underlying transport services i.e. transferred data volumes, time and reserved resources, signaling services like filtering, forwarding, scripting etc., storage devices like voice mail and gateway services like the above mentioned PSTN gateways. Furthermore, VoIP users may have an interest in receiving log Call Detail Records (CDRs) from VoIP systems for accounting or billing purposes. The standard way to accomplish this is with an external authentication, authorization, and accounting (AAA) server, e.g. a RADIUS service or a Terminal Access Controller Access Control System (TACACS, explained below). These AAA systems provide CDR logging, post call record processing, and a billing report generation facility.

The pre-mentioned RADIUS protocol is a client/server protocol that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to a requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It provides better security,

allowing a company to set up a policy that can be applied at a single administered network point. Having a central service also means that it's easier to track usage for billing and for keeping network statistics. TACACS is an older authentication protocol common to UNIX networks that allows a remote access server to forward a user's logon password to an authentication server to determine whether access can be allowed to a given system.

Beyond the pre-discussed prior art approaches, there exist VoIP solutions where IPT and plain (old) switching telephony network (PSTN) coexist. An according voice over data telecommunications network architecture is disclosed in WO 0031933 A1 where communicating voice and data over a packet-switched network that is adapted to coexist and communicate with the PSTN. Further EP 0966145 A2 describes an IP telephony gateway that provides communications between a PSTN and an IP network. The gateway can handle calls between clients on the SCN and IP clients on the IP network. The gateway also provides supplementary call services/features to calls between IP clients on the IP network. This is achieved by routing call control signaling for calls between IP clients via the gateway where the services can be controlled. In WO 0118703 A1 a mechanism for insuring correct transmission over the Internet through TCP/IP, Voice-over IP (VoIP) etc. that includes charging a fee to an appropriate account for a selected coverage type and amount is disclosed.

The above discussed known approaches disadvantageously do not provide a mechanism for managing access to and delivery of different electronic services based on service attributes like the above mentioned QoS levels in an above described IP based service delivery environment. In addition, there are not known

approaches, which prevent abuse or misuse of electronic services or an electronic service infrastructure. The only known approach for handling different service attributes, e.g. QoS levels, in an above mentioned B2C or B2B scenario is to map different QoS levels to different TCP port levels, e.g. known port '8080', the so-called "layer 4 switching". Only exemplarily, ports 80 (http) and 21 (ftp) can be used for services not requiring a certain QoS level e.g. Internet surfing and file-transfer. Port 554 (RTSP) can be used for services requiring a certain Quality-of-Service level in regard of jitter and delay time. Thus port 554, in the present example, can be used for services like Voice-over-IP (VoIP) and video streaming with a QoS level of '1' i.e. providing data streams with no jitter.

The drawback of the latter approach is that port-controlled service delivery in regard of QoS is rather difficult to implement in a service provider environment, where the client software resides on the customer's premises and therefore is controlled by the customer. In addition, ISPs have no means to accurately measure how their customers use services and network resources having different QoS levels and effectively bill for that usage.

In addition, the known approaches cannot provide service-oriented billing and prevention of misuse of the service delivery platform.

Further, the above-mentioned existing VoIP protocols and standards do not allow for reliable mapping charging or billing (tariff) models known from PSTN into an IP based telephone network.

SUMMARY OF THE INVENTION

It is thence an object of the present invention to provide a method and system for an improved and more reliable than the prior art approaches managing access and delivery Internet protocol (IP) packet based electronic services as described beforehand.

Another object is provision of an IP packet based telephony with improved quality of service handling capabilities.

It is yet another object to provide an improved mechanism for preventing unauthorized use of an electronic service and the electronic service environment/infrastructure, e.g. electronic services requiring a certain quality of service for the delivery to a service recipient.

Still another object is to provide a mechanism for enabling service-oriented billing.

These objects are attained by the features of the independent claims. Advantageous embodiments are subject matter of the subclaims.

The underlying idea of the invention is to separate electronic services requiring distinct set of service parameters (QoS levels, filters, etc.) by assigning certain quantities of IP addresses to different services or classes of services. That assignment of IP addresses can be statically or dynamically. If assigned statically, a certain IP address is assigned to a certain application, user or hardware device. Thus, depending on a requested service comprising a certain service attribute

or set of service attributes like QoS level(s), in particular the requested service enabling IP address is assigned or granted, e.g. from a pool of available IP addresses. A service-dependent filter or firewall rules can be used in particular for preventing misuse of an underlying e.g. cost-extensive service.

As an example, if an IP-telephone, as an user end device, is authenticated and a Network Access Server (NAS) gets/assigns its IP-address and a service-specific (here VoIP) set of attributes, the filters in this set of attributes prohibit direct data-connections (so-called 'peering') to other user end devices. Only IP-addresses belonging to the VoIP-Service universe are reachable (e.g. SIP-Proxy). Therefore it is impossible to use the cost-extensive QoS-enabled IP-Network for Internet browsing or peer-to-peer communication.

The proposed mechanism thus grants or denies access to a requested service or service infrastructure based on a currently assigned IP address. A service-dependent assigned IP address for a service with a defined QoS level guarantees that all data packets are transferred in a particular way and/or via a particular network infrastructure, also allowing full control of these data packets during transmission.

The concept of strictly assigning IP addresses to different services thus determines authorization for use of an electronic service insofar as an IP address reserved for e.g. video conferencing cannot be used for e.g. 'surfing' on the Internet and vice versa.

It is noted hereby that the assignment of an IP address to an e-client can be accomplished dynamically or statically using

the pre-discussed mechanism described in European Patent Application 01130600.8. In case of a dynamic assignment of the IP address, selection of the relevant e-service class can be done via a Media Access Control (MAC) address of the underlying user client device, an ATM VC, a Called-Station-ID (CSID) or Calling-Station-ID (CLID) and/or a user name. Hereby known protocol schemes like the known Dynamic Host Configuration Protocol (DHCP) which is a communications protocol that lets network administrators manage centrally and automate the assignment of IP addresses in an organization's network, like the known Lightweight Directory Access Protocol (LDAP) which is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet, or like the pre-mentioned RADIUS protocol can be utilized. In a network, the MAC address is a computer's unique hardware number. If a computer is connected to the Internet, a correspondence table relates the assigned IP address to the computer's physical MAC address e.g. on a local area network (LAN). The MAC address is used by a MAC sublayer of the Data-Link Layer (DLC) layer of an underlying telecommunication protocol. There is a different MAC sublayer for each physical device type. The other sublayer level in the DLC layer is the Logical Link Control sublayer.

In case of static assignment of the IP address, for a given quantity of IP addresses for which e-clients can be configured, the necessary assignment to the available e-service classes has already be done. It should be noted that the necessary amount of available IP addresses for performing the mechanism according to the invention is currently not critical and will even be no issue in case of future IPv6 address space.

If assigned dynamically, the selected service attribute controls how data packets to be transmitted are treated. For instance, it can be guaranteed that data packets belonging to a continuing data stream of a delivered electronic service like a transmitted VoIP stream are transmitted continuously thus avoiding that data packets are transmitted using different network paths using the above mentioned data packet labeling technique.

In another aspect of the invention, an e-service class N is assigned to a class M of e-clients, based on an appropriate IP address for that service class N. The e-client class includes all currently known and future devices that can principally be attached to IP networks. Hereby, according to another aspect, a single e-client can have assigned a number of IP addresses for different e-service classes. In addition, if defined in a corresponding e-service class, an e-client can use different services at the same time having assigned only one IP address. In such a scenario, the invention secures that the e-client cannot leave the currently using e-service class that is defined by the currently assigned IP address.

According to yet another aspect of the invention, the service class N is defined via parameters like backbone performance of the underlying network, an IP filter and/or network availability. The assignment of an IP address to an e-client can be represented as tuple (IP address, e-client) and is extended according to the invention by the e-service class. Hereby a strict relation between an e-service class N and an e-client is achieved.

In still another aspect, the service class N can be attributed

in order to enable a specific use of an e-service via an IP network. Exemplary attributes are applied IP filters, firewall rules or quality of service (QoS) i.e. the used bandwidth (network resources) for delivery of the service.

In another aspect, a one-to-one correlation of an e-client to an e-service domain effectively prevents misuse or abuse of the e-service.

In another aspect, the invention provides an entire solution for the pre-discussed accounting issue. Accounting information relevant for e-service events can be gathered and forwarded (redirected) within pre-selected e-service classes or the corresponding e-service applications like IP telephony, Web-TV, video conferencing, gaming, etc. for each e-client bank account.

In another aspect, service classes for all the available electronic services are managed utilizing the session context mechanism disclosed in European Patent Application 01130600.8. That mechanism thus effectively prevents misuse of a QoS-related IP address already assigned to a user's computer or other communication device.

The above mechanism can preferably be implemented as a managing or server instance (middleware) is arranged in the transport layer of the well-known ISO/OSI seven layer model for managing the underlying service instances.

The proposed mechanism thus advantageously enables a strict service oriented billing and management of service enabled QoS production environments like for example video-distribution and telephony based on IP.

Only exemplarily, the present invention allows to offer and thus produce classical POT services in carrier grade IP networks including an Internet service usage billing solution and to gather call information comparable to CDRs known from classical POT services. All known and potentially envisagable tariff models can be mapped like speech time units, far and near tariffs, etc. Further it provides compatibility to work with current/existing network and systems infrastructure i.e. any existing business process instances like customer care or customer self-care and accounting (billing) can be sustained without any modifications. Call information comparable to "call detail records" (CDRs) known from classical POT services can be gathered in order to provide exact telephone billing. The invention thus allows to alternatively offer and produce classical telephony services in carrier-grade IP networks.

The invention therefore enables step-wise conversion of PSTN services and/or systems into computer (IP)-based telephony. Any existing technology resources like billing, IP infrastructure etc., and any existing service architecture can be leveraged thus minimizing the required cost efforts for implementing IP telephony. In addition, existing customer databases or the like can be taken over and thus be used further without need of any changes.

Another advantage of the present invention is that misuse of a service, i.e. an unauthorized Internet client using a cost extensive service enabled infrastructure (concerning for example QoS and bandwidth) like VoIP telephony, is securely prevented.

The present invention can be applied in all electronic service arenas where IP packet based data streams are to be delivered in a digital network with limited data transmission bandwidth or resources with a given QoS level, including but not limited to IP telephony, video-on-demand, video conferencing services, or e-Mail services delivered on the Internet or any company proprietary Intranet.

It is noteworthy that the assignment of IP addresses to user clients, particularly the (continuing) static assignment of an IP address to a client device, will be easier in the future due to he forthcoming new IP protocol version 6 that provides a considerably larger IP address space than the currently used version. As a consequence, in the future IP addresses can be assigned to user clients with arbitrary granularity regarding the above-described assignment of service classes to clients.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention will be described in the following by way of a preferred embodiment. Hereby reference is made to the accompanying drawings. In the drawings,

Fig. 1 is an overview block diagram illustrating an IP telephony environment with two different IP networks (backbones) in accordance with the present invention;

Fig. 2A-C is a schematic view of three basic mechanisms for service-level or QoS-level dependent assignment of IP addresses according to the present invention;

Fig. 3A,B are further block diagrams illustrating two different modes for providing an IP connection of a client computer in accordance with the present invention;

Fig. 4A,B are further block diagrams illustrating two different ways for separation of IP data traffic dependent on service-level parameters in accordance with the present invention;

Fig. 5 is a block diagram illustrating a control mechanism for the data traffic on a single IP network (backbone) in accordance with the present invention;

Fig. 6 illustrates the basic principles for establishing a session context during an online session within an IP network in order to manage access to payable electronic services; and

Fig. 7 is an illustration of the known RADIUS protocol for providing authentication, authorization and configuration information between a Network Access Server (NAS) and a Shared Authentication Server.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

In Fig. 1, an Internet Protocol based telephony (IP telephony) environment is illustrated as one of a multitude of possible electronic services where the mechanism according to the invention can be used. It is emphasized that the shown IP telephony environment represents only a basic implementation comprising only minimum required hard- and software devices or

elements.

IP telephony (IPT), often referred to as "voice-over-IP" (VoIP), is used for voice delivered using the Internet Protocol (IP). VoIP, more particularly, is used as a set of facilities for managing the delivery of voice information using IP. In general, this means sending voice information in digital form in discrete packets rather than in the traditional circuit-committed protocols of the public switched telephone network (PSTN). A major advantage of VoIP and IPT is that cost-extensive switch technology used by ordinary telephone service can be avoided.

In addition to common IP-services like for example http and ftp, VoIP uses a real-time protocol (RTP/RTSP) to help ensure that packets get delivered in a timely way. But using public networks, it is currently difficult to guarantee Quality of Service (QoS). On the Internet and in other networks, QoS is the idea that transmission rates, error rates, and other characteristics can be measured, improved, and, to some extent, guaranteed in advance. QoS is of particular concern for the continuous transmission of high-bandwidth video and multimedia information including voice in a telephony environment. Transmitting this kind of content dependably is difficult in public networks using ordinary "best effort" protocols. Better service is possible with private networks managed by an enterprise or by an Internet telephony service provider (ITSP).

In the IPT environment shown in Fig. 1, two exemplary user hardware devices 100, 110, the first user device 100 being a common Personal Computer (PC) and the second one 110 being a VoIP telephone device, which both are connected to a Digital

Subscriber Line (DSL) modem 120. It is emphasized that the shown user devices 100, 110 are only exemplary and can principally be also two PCs or devices usable for VoIP.

The above-mentioned DSL technology is known in the art for providing high-bandwidth information to homes and small businesses over ordinary copper telephone lines. There exist different variations xDSL of the mentioned DSL, such as ADSL, HDSL, and RADSL which all can be used in the present environment. A DSL service allows to receive data at rates up to 6.1 megabits (millions of bits) per second (of a theoretical 8.448 megabits per second), enabling continuous transmission of motion video, audio, and even 3-D effects. More typically, individual connections will provide from 1.544 Mbps to 512 Kbps downstream and about 128 Kbps upstream. A DSL line can carry both data and voice signals and the data part of the line is continuously connected.

The DSL modem 120 itself is connected via line 125 to a Digital Subscriber Line Access Multiplexer (DSLAM) 140 which is a network device, usually at a telephone company central office, that receives signals from multiple customer DSL connections and puts the signals on a high-speed backbone line using multiplexing techniques. At a local level, a 'backbone' is a line or set of lines that local area networks connect to for a wide area network connection or within a local area network to span distances efficiently (for example, between buildings). On the Internet or other wide area network, a backbone is a set of paths that local or regional networks connect to for long-distance interconnection. The connection points are known as network nodes or telecommunication data switching exchanges (DSEs).

In the present environment, the DSLAM 140 connects the DSL line 125 with a Network-Access-Server (NAS) 170.
The NAS 170 splits the data traffic and tunnels it to the LNS connected to the corresponding network. As one can see, the best effort data packets from the PC 100 are forwarded to the LNS 180 - logical connection 130. The QoS-Traffic from the VoIP phone is forwarded to the LNS 190, which is connected to the QoS-Backbone - logical connection 135.

A NAS is a router that enables an independent or Internet service provider (ISP) to provide connected customers with Internet access. The NAS has interfaces to both the local telecommunication service provider such as a telephone company and to the Internet backbone (see above). The router authenticates users requesting login. It receives a "dial-up" call from each user's client computer or device that wants to access the Internet, performs the necessary steps to authenticate and authorize each user, usually by verifying a user name and password, and then allows requests to begin to flow between the user host and hosts (computers) elsewhere on the Internet.

It is noteworthy that the connection between the telephony end user device 110 and the NAS 170 is a Point-to-Point Protocol (PPP) connection whereby PPP packets are exchanged. The PPP is a protocol for communication between two computers using a serial interface, as in the present case, a PC connected by telephone line to the NAS server. The PPP connection enables the NAS server to respond to any requests delivered by the end users and forward the requested responses back to the end users. IP uses the PPP protocol. Relative to the Open Systems Interconnection (OSI) reference model, PPP provides layer 2 (data-link layer) service.

The shown two LNS servers 180, 190 terminate the exchanged PPP packets and turn them into IP packets. The LNS servers 180, 190 can also be implemented in one network router. In addition, the dotted line 150 shall indicate that the NAS server 170 and the exemplarily two local LNS servers 180, 190 can also be implemented in a single network router.

The LNS servers 180, 190, in particular, handle the assignment of IP addresses to the end user's devices. The assignment, in accordance with the present invention, is accomplished in dependence on QoS related attribute values, as described in more detail hereinafter. In the present example, the first LNS server 180 is used to assign IP addresses without any special service attributes (e.g. QoS, filters,...), i.e. IP addresses e.g. used only for accessing the Internet. In contrast to that, the second LNS server 190 is used to assign IP addresses with a certain QoS level. As a consequence, the two LNS servers 180, 190 are connected to two different, logically or physically separated networks 200, 210. Due to the QoS requirements of the second LNS server 190, the second network 210 accordingly is QoS-enabled network like an Asynchronous Transfer Mode (ATM) or MPLS network. ATM is a dedicated-connection switching technology that organizes digital data into 53-byte cell units and transmits them over a physical medium using digital signal technology. Individually, a cell is processed asynchronously relative to other related cells and is queued before being multiplexed over the transmission path. Because ATM is designed to be easily implemented by hardware (rather than software), faster processing and switching speeds are possible.
MPLS is a Multi-Protocol-Label-Switching network where "IP-packets" are switched but not routed.

Referring to Figures 2A to 2C, the basic concept of the mechanism for assignment of service or service attributes, in the present example QoS-related, IP addresses is illustrated. The mechanism is mainly based on two class definitions IP_User (or IP_User_End_Device) and IP_Service. In the present example, the possible attribute of class IP_User is 'user_account' wherein the possible attributes of IP_Service are 'QoS' and 'filters'.

It is emphasized that the class definition IP_User_End_Device represents the underlying service platform like Web-TV, Web-Radio or VoIP. The described class definition concept can also be implemented by way of different Uniform Resource Locators (URLs) commonly used as IP address for Internet end users. The following are exemplary URLs for illustrating such an implementation. It is noted that each of the following URLs is determining a different set of attributes, as mentioned beforehand.

a) The following URL

username@serviceprovider.com

is fixedly assigned with an attribute set A where the QoS level is 'low' and the filter is 'unlimited' and thus the assigned IP address can be used for all kinds of IP services but with low QoS.

b) The URL

username@phone.serviceprovider.com

has assigned an attribute set B with a QoS level 'high' and filter set to 'VoIP platform'. The filter guarantees that the end user can use that IP address only for VoIP services, which require a high QoS and thus have to be handled via a high bandwidth transmission network.

c) The URL

username@QOSsurf.serviceprovider.com

has assigned an attribute set C with a QoS level 'high' and filter 'unlimited' and thus can be used for all kinds of IP services like Internet surfing, WebTV, Video-on-Demand and other services requiring high bandwidth for the transmission of the IP packets.

It should be mentioned that the above capital letter notation for 'QOS' is only for illustration purposes.

In the IP assignment mechanism illustrated in Fig. 2A, there are provided different IP addresses for different services, as in the present example IP 1, IP 2, ... IP 10 for services of the class 'Service_1', IP 11 and IP 12 for services of class 'Service_2', IP 14, IP 15, ..., IP 18 for services of class 'Service_n', etc.. Further it is presumed that each user end device shall only be used for a distinct service, e.g. a VoIP telephone for making phone calls and/or a common PC for surfing on the Internet, and thus each user end device is assigned a fixed IP address corresponding to the respective underlying service or service class. Due to the static and fixed assignment of IP addresses, the shown IP assignment mechanism is performed preferably on a network router itself.

In Fig. 2B, another embodiment is shown where each service class 'Service_1' to 'Service_n' is assigned a fixed pool of IP addresses, in the present example IP 1, IP 2, ..., IP 100 for class 'Service_1', IP 101 and IP 102 for class 'Service_2' and IP 800, IP 801, IP 802, ..., IP 1000 for class 'Service_n'. The assignment of the IP addresses will be implemented preferably in a middleware communicating with the Network Access Router.

Fig. 2C shows still another embodiment where IP addresses are assigned dynamically dependent on both the respective service itself and the service platform i.e. the underlying user end device. Hereby a network router provides a pool of available (routed) IP addresses IP 1, IP 2, ..., IP 1000. According to the scenario disclosed in European Patent Application 01130600.8, the mechanism is implemented in a middleware that communicates with the network router and assigns an IP address and sends control filters 'm' and QoS-level to the NAS. The network access router, in the present example, assigns IP address IP 80 out of said pool of available IP addresses to the user end device. The middleware (MW) stores the triple (IP 80, QOS:1, Filter:m). Dependent on the three parameters or value of these parameters, respectively, the delivered IP packets (IP traffic) for fulfilling the requested service will be routed via an IP network comprising the necessary transmission resources, e.g. an MPLS network in vase of Video-on-Demand or VoIP, as mentioned beforehand.

In case of a dynamic assignment of IP addresses, an appropriate service class N can be selected dependent on user client device characteristics like the MAC address.

In Figures 3A and 3B two different embodiments for connecting user end devices to one or more data transmission networks,

which support different electronic services and related different QoS levels, are illustrated. It is assumed herein that delivery of services with different service parameters like the QoS level or filtering level can be separated strictly from each other.

Fig. 3A shows a Point-to-Point Protocol over Ethernet (PPPoE) connection with multiple (in the present case two) e-clients 300, 310, i.e. multiple sessions are handled via only one network access server (NAS). The PPPoE is a specification for connecting multiple computer users on an Ethernet local area network to a remote site through common customer premises equipment i.e. a modem and similar devices. Hereby multiple IP addresses are assigned. The PPPoE can be used to have an office or building-full of users share a common Digital Subscriber Line (DSL), cable modem, or even wireless connection to the Internet. PPPoE combines the Point-to-Point Protocol (PPP), commonly used in dialup connections, with the Ethernet protocol, which supports multiple users in a local area network. The PPP protocol information is encapsulated within an Ethernet frame.

The PPPoE has the advantage that neither the telephone company nor the Internet service provider (ISP) needs to provide any special support. Unlike dialup connections, DSL and cable modem connections are "always on". Since a number of different users are sharing the same physical connection to the remote service provider, a way is needed to keep track of which user traffic should go to and which user should be billed. PPPoE provides for each user-remote site session to learn each other's network addresses (during an initial exchange called "discovery"). Once a session is established between an individual user and the remote site (for example, an Internet

service provider), the session can be monitored for billing purposes. Many apartment houses, hotels, and corporations are now providing shared Internet access over DSL lines using Ethernet and PPPoE.

In Fig. 3a, the two e-clients 300, 310, are connected via a DSL modem 320 and a DSLAM 330 to a NAS 340 via the mentioned PPPoE connection. The PPPoE connection can be a XDSL connection. Each e-client initiates an own PPP session via the DSL modem and the NAS and obtains during the necessary Link Control Protocol (LCP) negotiations an IP address corresponding to the requested electronic service together with the required set of attributes, the attributes controlling e.g. the QoS level or IP filters used for the service delivery.

The mentioned LCP establishes, configures, and tests data-link Internet connections. Before establishing the communication over the mentioned point-to-point link, each end of the PPP link, i.e. the respective e-client and the NAS in the present example, must send out LCP packets. An LCP packet either accepts or rejects the identity of its linked peer, agrees upon packet size limits, and looks for common misconfiguration errors. Basically, an LCP packet checks the telephone line connection to see whether the connection is good enough to sustain data transmission at the intended rate. Once the LCP packet accepts the link, traffic can be transported on the network; if the LCP packet determines the link is not functioning properly, it terminates the link.

LCP packets are divided into three classes:

1. Link configuration packets used to establish and configure a link

2. Link termination packets used to terminate a link

3. Link maintenance packets used to manage and debug a link

Exemplary connections of the NAS are discussed in greater detail referring to Figures 4A - 5.

In Fig. 3B another embodiment is illustrated where two e-clients 410, 420 are connected to a QoS backbone 430 via the edge routers 440. The edge router 440 maintains a pool of available IP addresses IP1 - IPn. It is hereby assumed that the e-client devices 410, 420 are statically connected to the edge routers 440 and that the edge router 440 provides a pool of fixed IP addresses.

The IP addresses available on side of the edge routers 440have assigned different sets of attributes 460, 470 for controlling delivery of the underlying services. These sets of attributes 460, 470, in the present embodiment, include the QoS level for service delivery to the e-clients, an IP filter assuring the use of the related service only corresponding to the respectively underlying IP address.

In the embodiment illustrated in Fig. 3B it is further assumed that the backbone 430 comprising the edge router(s) is fully QoS enabled what means that there is not required to split data traffic dependent on the underlying QoS level for data transmission. In other words, the service parameters, in the present embodiment the QoS level and IP filter, are fixedly coupled with an IP address. The assignment of a IP address and thus of an electronic service to a single e-client can be performed by way of configuration based on e-client device parameters like the pre-mentioned MAC address or a virtual

circuit (VC) in Asynchronous Transfer Mode (ATM) networks. The connection of one or more networks to the edge router(s) is illustrated in the following referring to Fig. 4B and Fig. 5.

Fig. 4A shows an embodiment, where the e-client's session, depending on the pre-mentioned criteria (e.g. username, MAC-address, VC, CLID, CSID, ...) is tunneled from the NAS 500 to its service specific Tunnelendpoint (LNS) 510, 520, where the client gets its service-class dependant IP-address, a set of attributes (e.g. QoS-Level, filters ...). The specific LNS 510, 520 is connected to a particular network 530, 540, providing the requested service. For example "Best Effort" 540 for Internet surfing and QoS enabled network 530 transport for IP-Telephony and Video-Streaming.

Fig. 4B shows an embodiment, where an e-client gets its IP-address and set of attributes (e.g. QoS-Level, filters, ...) dependent on the pre-mentioned criteria (e.g. username, MAC-address, VC, CLID, CSID, ...). According to the (statically or dynamically) assigned IP-address and therefore accordingly assigned service/service-environment, the data-packets are routed to the QoS-Backbone or the "Best Effort" Backbone. This means a splitting of the service data traffic on OSI-Layer3 basis.

Referring now to Fig. 5, it is shown a NAS connected to a fully QoS-enabled backbone. Depending on the pre-mentioned criteria (e.g. username, MAC-address, VC, CLID, CSID, ...) the NAS gets an IP-address and the set of attributes according to the "requested" service. The NAS, for example, then sets the QoS-Level for the data packets and the filters according to the information in the set of attributes.

From a more abstract point of view, a service class N is assigned to a class M of clients based on an appropriate IP address for that service class N. The client class M, in the present IP telephony environment, includes specifications of known devices like IP telephony applications to be run on a conventional client computer or a digital telephone device, i.e. all devices that can principally be attached to IP networks. In addition, specifications of not yet existing future devices can be included.

The shown single client, in the present embodiment, has assigned a number of IP addresses for different service classes N, N', ... However, if defined in a corresponding service class N', a client alternatively can use different services at the same time having assigned only one IP address. In such a scenario, the present IP address and the filter assignment mechanism secures that such a client cannot leave the currently using service class that is defined by the currently assigned IP address.

The service class N, in the present embodiment, is defined by the parameters backbone performance of the underlying network and the network availability. In addition, one or more filters applied by the NAS can be used for that service class. The assignment of an IP address to the client is represented herein as a tuple (IP address, client) and is extended by the above mentioned service class N. Hereby a strict relation between a service class N and a corresponding client is achieved.

Further, the service class N is attributed in order to enable only a specific use of a service via an IP network. Exemplary attributes, which can be applied, are IP filters, firewall

rules or quality of service (QoS) i.e. the used bandwidth (network resources) for delivery of the underlying service.

As mentioned beforehand, the achieved strict one-to-one relation of a client to a service domain already prevents misuse or abuse of the service. In order to more effectively prevent misuse of an already assigned QoS-related IP address, the Authentication, Authorization and Accounting (AAA) mechanism described in pre-cited European Patent Application 01130600.8 can be applied also in the present environment. Thus in Fig. 6, the basic principles of how to establish a session context within an IP network are illustrated. In addition, it is illustrated how to provide electronic services and track all relevant accounting information and billing parameters based on dedicated service characteristics. In the diagram, the y direction, starting from the top, represents the time t, and the two vertical lines 300, 302 arranged in the x direction, represent to different transaction contexts, in the present example particularly to the pre-described session context and, in addition, one sales entity context.

The process begins with a sign-on procedure (step 'a') by the user, which includes user authentication, as described beforehand. An IP address is assigned and a session context is created using the known RADIUS protocol described in more detail by way of Fig. 7. A session context records RADIUS-provided information like: Username, Framed-IP-Address and Class, Acct-Session-ID. The session context expires, when the user signs (logs) out or is disconnected.

Only during a pending session context, other transaction events initiated by the user or any e-service provider being involved in a business transaction can principally occur

wherein the session context is confirmed (step 'b'). The moment a user orders a sales-entity, an Authorization-Request is sent (step 'c'') to the server instance. The middleware validates the user's sales-entity request and grants that the user is liable for these costs. A so-called sales-entity context is generated (step 'c). In the present example, the user requests a video-on-demand service from the e-service provider. After his successful authorization (step 'c''), the start of the requested video-on-demand (VoD) service is indicated (step 'd') with an Accounting-Message (Acct-Start). When the VoD-service is finished, e.g. having downloaded or streamed the complete video file, an Accounting-Message (Acct-Stop) is generated in order to conduct the necessary billing for the downloaded video. The pending sales-entity context is deleted (step 'f').

When the user signs off, the recorded session context is deleted and the pending IP address de-allocated. Further an accounting-stop event is triggered (step 'g'). Any special service-event like rewind, pause/resume or forward the video during the streaming, will trigger an Accounting-Message (Acct-Intermediate).

The described session context is maintained by the proposed middleware. Any service layer will interface to the middleware in terms of service authorization and accounting.

Referring finally to Fig. 7, the previously mentioned RADIUS (Remote Authentication Dial In User Service) protocol, published e.g. in RFC2865, RFC2866, RFC2867 and RFC2868 (www.ietf.org) is described in more detail.

The RADIUS protocol sets out a method of carrying out

authentication, authorization and configuration information between a Network Access Server (NAS) 400 and a Shared Authentication Server. A first key feature of RADIUS is the underlying Client/Server Model where a Network Access Server (NAS) operates as a client of RADIUS. The client is responsible for passing user information to designated RADIUS servers 402, and then acting on the response that is returned. In contrast to that, RADIUS servers are responsible for receiving user connection requests, authenticating the user, and then returning all configuration information necessary for the client to deliver service to the user. A RADIUS server can act as a proxy client to other RADIUS servers or other kinds of authentication servers.

It should be mentioned that communication between a NAS and a RADIUS server is based on the known User Datagram Protocol (UDP). UDP, documented in protocol standard RFC 768, provides users access to IP-like services. UDP packets are delivered just like IP packets - connection-less datagrams that may be discarded before reaching their targets. UDP is useful when TCP would be too complex, too slow, or just unnecessary. More particularly, UDP is defined to make available a datagram mode of packet-switched computer communication in the environment of an interconnected set of computer networks. This protocol assumes that the Internet Protocol (IP) is used as the underlying protocol. UDP is mainly used in application programs to send messages to other programs with a minimum of protocol mechanism. The protocol is transaction oriented, and delivery and duplicate protection are not guaranteed. Applications requiring ordered reliable delivery of streams of data should use the Transmission Control Protocol (TCP).

The above mentioned authentication request message contains the user-supplied name and password, as well as the identity of the access device sending the request and the port being used for the remote connection. Since communication with the RADIUS server occurs across the network, the user-supplied password is typically encrypted by the NAS before the authentication request is sent to minimize the chance for compromise.

The authentication request can be sent to either a "local" RADIUS server via the local area network or to a "remote" server over a wide area network. This provides flexibility in designing the overall network architecture by allowing placement of the RADIUS server at the most appropriate location, not necessarily at the physical point of remote access. This is an important feature in cases where a "host" organization must maintain control of the authentication process but wishes to outsource most or all other elements of the remote access infrastructure. The RADIUS protocol also facilitates authentication redundancy by allowing the client devices to route requests to alternative servers if the primary RADIUS server cannot be reached.

When the RADIUS server receives the authentication request, it validates the request (to ensure it originated from a valid client device) and then decrypts the data packet to expose the user name and password. These credentials are then passed to the system being used to conduct the authentication process. The information used to authenticate the user sign-on (log-on) request can be contained in a password file, centralized authentication database, or a custom (or proprietary) system. Other commercial security systems (e.g., Kerberos) that

support the RADIUS protocol can also be interfaced with to provide authentication.

If the credentials (name and password) of the user requesting access are properly matched against the stored information, the RADIUS server returns an authentication acknowledgement message to the NAS. This message contains the connection information (network type and services) necessary for attaching the authenticated user to the network. Hence, the type of connection (TCP/IP, PPP, SLIP, etc.) and access restrictions are applied to the user's login in accordance with pre-established policies. In the opposite case, if the credentials received from the RADIUS client do not match information in the authentication information store, the server returns an authentication reject message to the NAS. This message causes the NAS to deny access to the user requesting it.

In addition to the encryption of the user password during communications between the NAS and the authentication server, the RADIUS protocol also provides for additional security to avoid compromise of authentication via tampering with the message transfer process. As mentioned above, the messages passed between RADIUS clients and servers are validated to prevent "spoofing" of these requests. The RADIUS server accomplishes this by sending an authentication key to the RADIUS client devices. This message acts as a digital signature to ensure that the proper authentication server is truly originating authentication messages.

The RADIUS protocol thus provides a high level of network security since transactions between the client and RADIUS server are authenticated through the use of a shared "secret",

which is never sent over the network. In addition, any user passwords are sent encrypted between the client and RADIUS server, to eliminate the possibility that someone snooping on a non-secure network could determine a user's password.

In addition, RADIUS provides flexible authentication mechanisms since the RADIUS server can support a variety of methods to authenticate a user. It can support PPP PAP or CHAP, UNIX login, and other authentication mechanisms. Last but not least RADIUS is a highly extensible protocol since all transactions are comprised of variable length Attribute-Length-Value 3-tuples. New attribute values can be added without disturbing existing implementations of the protocol.

Concerning authentication and authorization, the RADIUS server 402 can support a variety of methods to authenticate a user. When it is provided with the username and original password given by the user, it can support PPP, PAP or CHAP, UNIX login, and other authentication mechanisms. Typically, a user login consists of a query (Access-Request) from the NAS to the RADIUS server 402 and a corresponding response (Access-Accept or Access-Reject) from the server. The Access-Request packet contains the username, encrypted password, NAS IP address, and additional information of the type of network connection.

When the RADIUS server 402 receives the Access-Request from the NAS, it searches a database for the username listed. If the username does not exist in the database, either a default profile is loaded or the RADIUS server 402 immediately sends an Access-Reject message. This Access-Reject message can be accompanied by a text message indicating the reason for the refusal.

The RADIUS accounting functions allow data to be sent at the start and end of sessions, indicating the amount of resources (such as time, packets, bytes, and so on) used during the session. An Internet service provider (ISP) might use RADIUS access control and accounting software to meet special security and billing needs.

The information technology (IT) based process or service according to the invention, in terms of the (OSI) model, preferably is implemented beyond an IP layer as a server instance or middleware of a server, as being illustrated in Fig. 6. It can be seen from Fig. 6 that the process is based on an interaction scenario comprising four main components, an e-Network Provider 500 providing the basic network infrastructure and backbone for executing the underlying communication protocols, one or more e-service Providers 502 which a (not shown) user is interested to do any kind of commercial or even non-commercial business (es), an e-Company 504 for managing the entire process and a middleware 506 arranged on top of the network infrastructure for processing a so-called "session context" as described in more detail hereinafter and for providing AAA control facility and sales entity management for conducting the pre-mentioned businesses in accordance with the novel business process according to the invention.

Although the invention has been described above in a VoIP environment, it can principally be applied to all fields of delivery of electronic services where delivery and provisioning of these services to a service recipient strongly depends on certain service attributes.

CLAIMS

1. A method for controlling access to and delivery of electronic services in an Internet protocol (IP) operated digital network environment, characterized in that electronic services requiring at least one service parameter or set of service parameters are separated by assigning certain quantities of IP addresses to different of said electronic services or to different classes of said electronic services.

2. Method according to claim 1, wherein assigning said certain quantities of IP addresses to said electronic services or classes of electronic services dependent on said at least one service parameter or set of service parameters.

3. Method according to claim 1 or 2, wherein assigning dynamically said certain quantities of IP addresses out of a pool of available IP addresses.

4. Method according to claim 3, wherein a selected service attribute controls how data packets to be transmitted are treated.

5. Method according to claim 1 or 2, wherein assigning statically said certain quantities of IP addresses, whereby a certain IP address is assigned to a certain application, user or hardware device.

6. Method according to any of the preceding claims, wherein said service parameters are Quality-of-Service levels, filters, or the like.

7. Method according to any of the preceding claims, wherein providing a service-dependent filter or firewall rules, in particular for preventing misuse of an underlying service.

8. Method according to any of the preceding claims, wherein assigning a service class N to a client class M is based on at least one appropriate IP address for the service class N.

9. Method according to any of the preceding claims, wherein said service class N is defined via network performance parameters or an IP filter/firewall rules.

10. Method according to any of the preceding claims, wherein assignment of an IP address to a client is represented by the triple (IP address, client class, service class).

11. Method according to any of the preceding claims, wherein said service class N is attributed to enable a specific use of an underlying service.

12. Method according to any of the preceding claims, wherein managing the access to and delivery of said electronic services or service classes based on session context information.

13. Method according to claim 12, wherein said session context information includes a Username and/or a Framed-IP-Address and/or a service class and/or an Account-Session-ID.

14. Method according to any of claims 8 to 13, wherein said service class N is automatically determined by a client-specific identifier, preferably the MAC address.

15. Method according to any of claims 8 to 14, wherein said service class N is automatically determined by the type of application running on side of the client.

16. Method according to any of claims 8 to 15, wherein said service class N is determined by a user interaction, preferably by means of a graphical user interface (GUI) button.

17. Method according to any of the preceding claims, wherein delivery of a service is billed using said assigned IP address and/or said service class N.

18. A method for establishing an Internet Protocol (IP) based telephone connection between a calling party and at least a called party, wherein said IP based telephone connection provides at least two voice quality levels, characterized in that

the calling party selects one of said at least two voice quality levels;

a certain IP address is assigned to the calling party dependent on the selected voice quality level; and

said telephone connection is established based on said assigned IP address and said selected voice quality level.

19. Method according to claim 18, wherein IP addresses available for said assignment are mapped on a certain billing structure for billing said telephone connection.

20. Method according to claim 18 or 19, wherein said certain IP address is assigned to a certain telephony application, user or telephone device.

21. Method according to any of claims 18 to 20, wherein providing a voice quality level-dependent filter, in particular for preventing misuse of said telephone connection.

22. Method according to any of claims 18 to 21, wherein said telephone connection is established based on session context information.

23. Method according to claim 22, wherein said session context information includes a Username and/or a Framed-IP-Address and/or a service class and/or an Account-Session-ID.

24. Method according to any of claims 18 to 23, wherein the calling party selects one of said at least two voice quality levels by means of a graphical user interface (GUI).

25. Method according to any of claims 18 to 24, wherein said telephone connection is billed using said assigned IP address and/or said voice quality level.

26. A computer program product stored on a computer usable medium, comprising computer readable program means for

causing a computer or communication device to perform the method according to anyone of claims 1 to 17 or anyone of claims 18 to 25.

27. A system for controlling access to and delivery of electronic services in an Internet protocol (IP) operated digital network environment, characterized by a method according to any of claims 1 to 17.

28. System according to claim 26, comprising a server for assigning certain quantities of IP addresses to different of said electronic services or to different classes of said electronic services for electronic services requiring at least one service parameter or set of service parameters.

29. Telephony system for an Internet protocol (IP) operated digital network environment, characterized by a method according to any of claims 18 to 25.

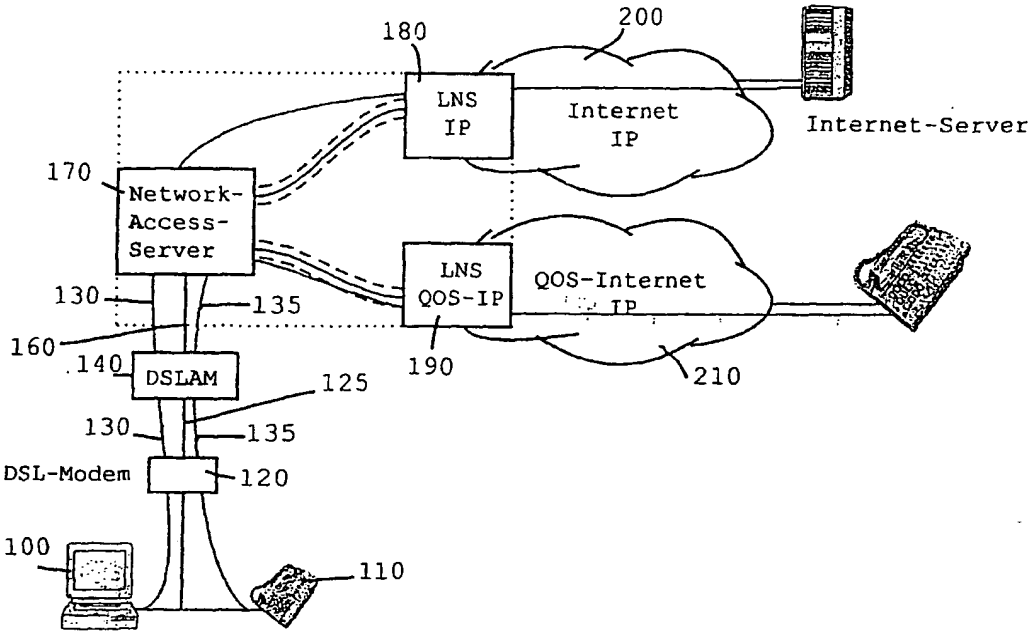


FIG. 1

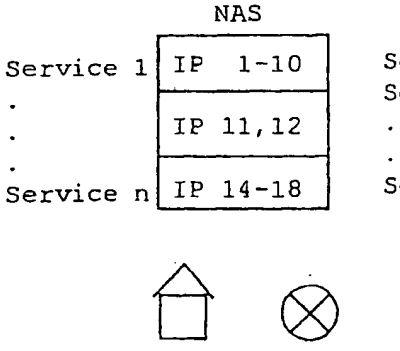


FIG. 2A

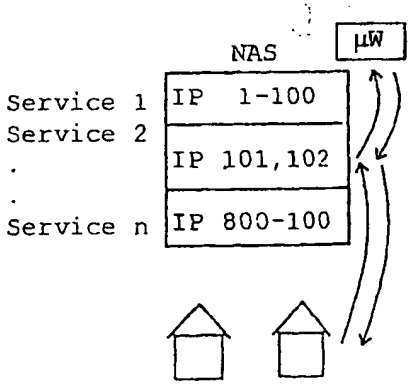


FIG. 2B

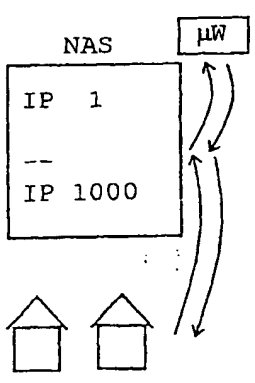


FIG. 2C

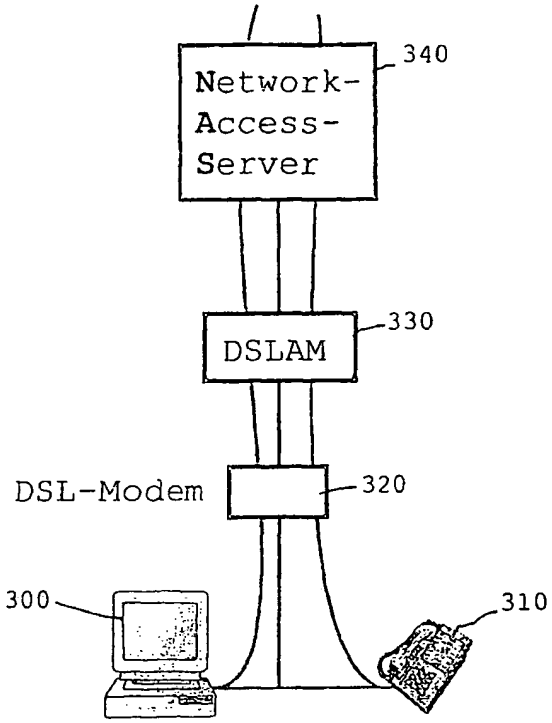


FIG.3A

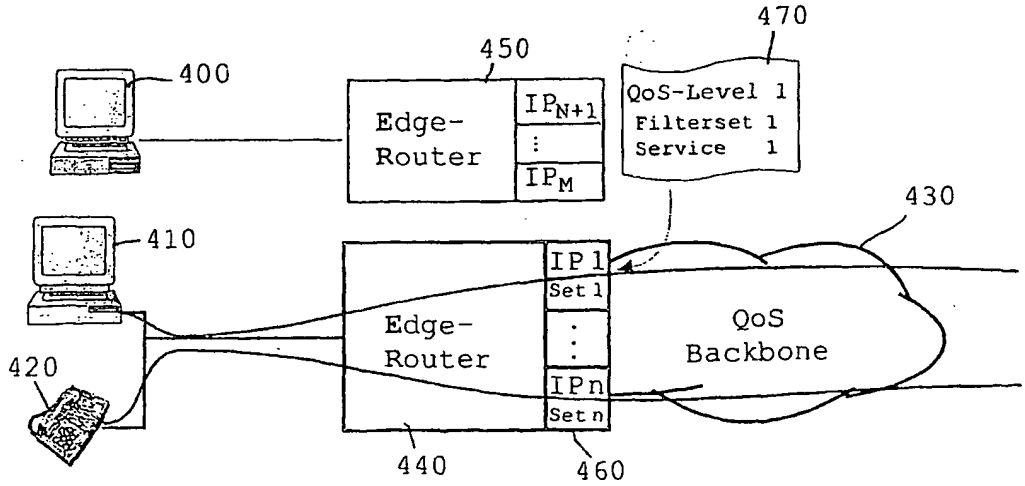


FIG. 3B

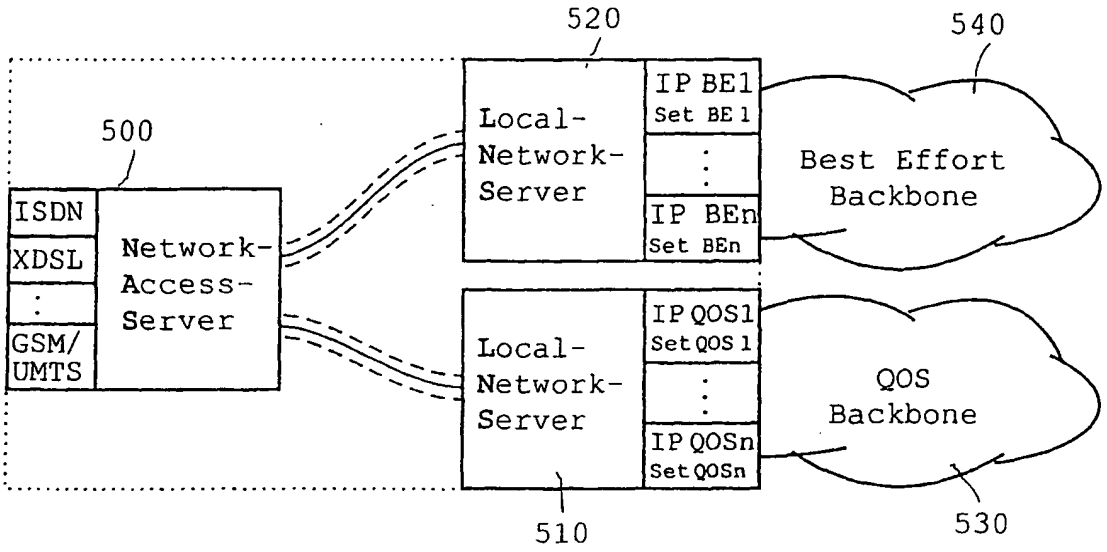

520
540
500
ISDN
XDSL
GSM/
UMTS
Network-
Access-
Server
Local-
Network-
Server
IP BE1
Set BE 1
IP BEn
Set BEn
Best Effort
Backbone
Local-
Network-
Server
IP QOS1
Set QOS 1
IP QOSn
Set QOSn
QOS
Backbone
510
530

FIG. 4A

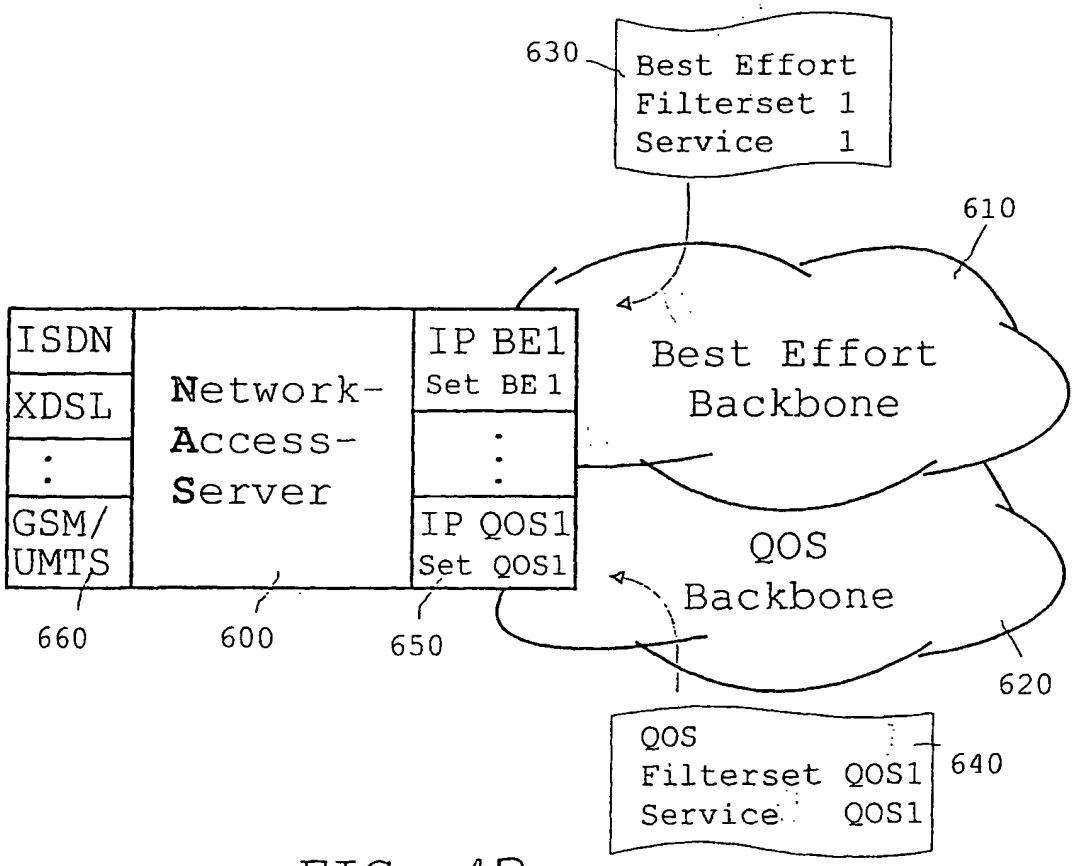

630
Best Effort
Filterset 1
Service 1
610
ISDN
XDSL
GSM/
UMTS
Network-
Access-
Server
IP BE1
Set BE 1
IP QOS1
Set QOS1
Best Effort
Backbone
QOS
Backbone
660
600
650
620
QOS
Filterset QOS1
Service QOS1
640

FIG. 4B

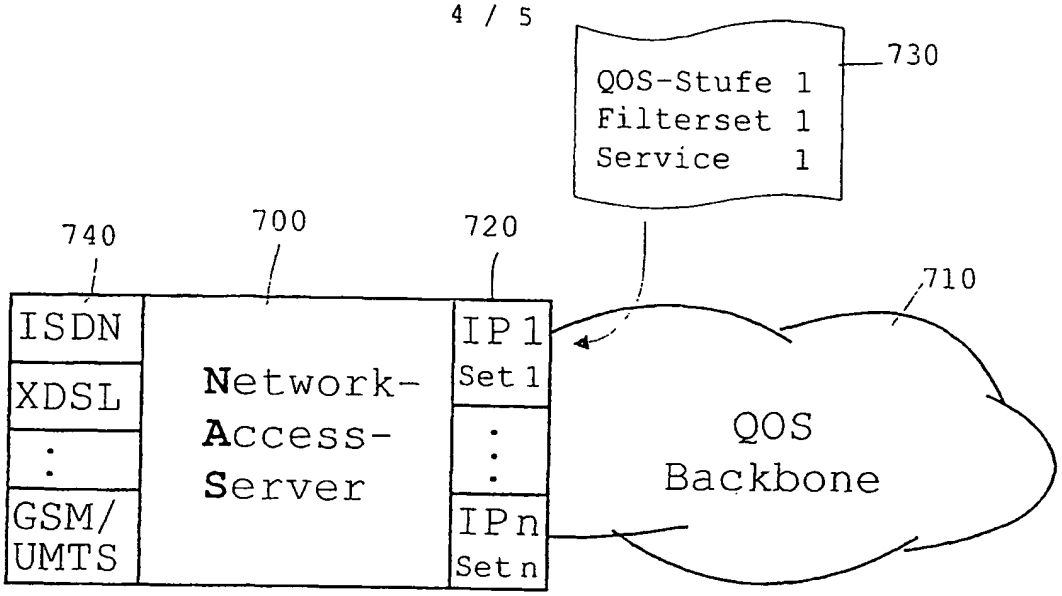

QOS-Stufe 1
Filterset 1
Service 1
730
740
700
720
710
ISDN
XDSL
GSM/
UMTS
Network-
Access-
Server
IP 1
Set 1
IPn
Set n
QOS
Backbone

FIG. 5

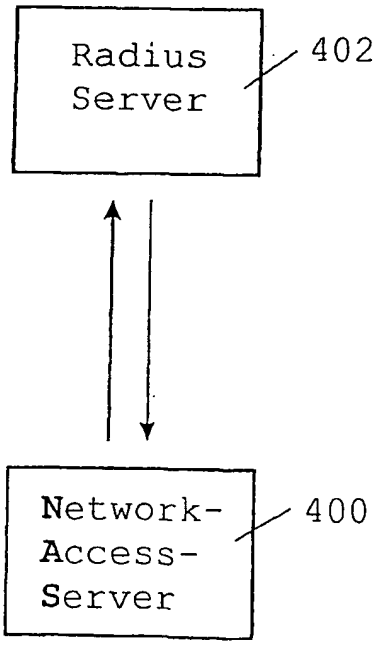

Radius
Server
402
Network-
Access-
Server
400

FIG. 7

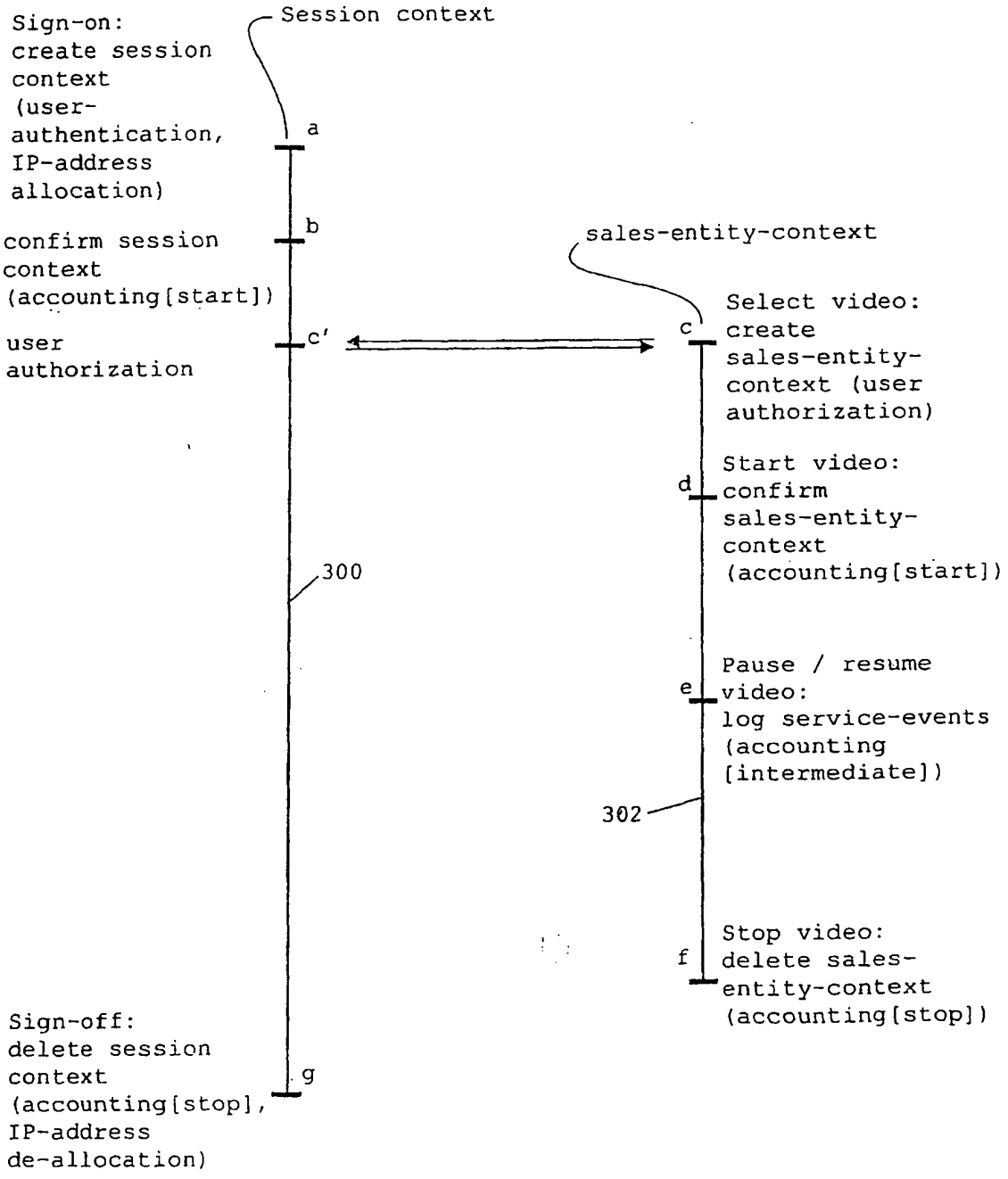

Session context
Sign-on:
create session
context
(user-
authentication,
IP-address
allocation)
a
b
confirm session
context
(accounting[start])
user
authorization
c'
sales-entity-context
c
Select video:
create
sales-entity-
context (user
authorization)
d
Start video:
confirm
sales-entity-
context
(accounting[start])
300
e
Pause / resume
video:
log service-events
(accounting
[intermediate])
302
f
Stop video:
delete sales-
entity-context
(accounting[stop])
Sign-off:
delete session
context
(accounting[stop],
IP-address
de-allocation)
g

FIG. 6

INTERNATIONAL SEARCH REPORT

Internatio[redacted] Application No
PCT/EP 03/07544

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/12 H04L29/06 H04L12/14

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2002/023174 A1 (KALMANEK CHARLES ROBERT ET AL) 21 February 2002 (2002-02-21)	1-16,18, 20-24, 26-29
Y	paragraphs '0002!,'0004!,'0006! paragraphs '0021!,'0025!,'0026! paragraphs '0034!,'0037! paragraphs '0042!,'0043!	17,19,25
X	WO 00 54477 A (BLOM MARCUS ANTHONIUS ;KONINKL KPN NV (NL)) 14 September 2000 (2000-09-14) abstract; claim 1 page 3, line 33 -page 4, line 12	1-11, 26-28

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 October 2003	24/10/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Losseau, D

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 03/07544

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 02 19585 A (VERIZON COMM INC) 7 March 2002 (2002-03-07)	17,19,25
A	abstract page 10, line 13-22 page 13, line 3 -page 14, line 15 page 15, line 4-11 page 20, line 21-25 page 21, line 3-11 page 29, line 30 -page 30, line 9 page 30, line 22 -page 31, line 8	12,13, 18-25,29

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP 03/07544

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2002023174 A1	21-02-2002	AU 4586801 A	03-10-2001
		AU 4590301 A	03-10-2001
		AU 4759001 A	03-10-2001
		AU 4763001 A	03-10-2001
		AU 5088801 A	03-10-2001
		AU 8725701 A	03-10-2001
		CA 2403625 A1	27-09-2001
		CA 2403628 A1	27-09-2001
		CA 2403733 A1	27-09-2001
		CA 2403736 A1	27-09-2001
		CA 2403765 A1	27-09-2001
		CA 2403832 A1	27-09-2001
		EP 1266488 A2	18-12-2002
		EP 1266508 A1	18-12-2002
		EP 1266489 A1	18-12-2002
		WO 0171567 A1	27-09-2001
		WO 0172013 A1	27-09-2001
		WO 0171982 A1	27-09-2001
		WO 0171983 A1	27-09-2001
		WO 0172003 A2	27-09-2001
		WO 0171984 A1	27-09-2001
		US 2001049737 A1	06-12-2001
		US 2001028660 A1	11-10-2001
		US 2001049729 A1	06-12-2001
		US 2002019875 A1	14-02-2002
		US 2002023171 A1	21-02-2002
		US 2002038419 A1	28-03-2002
		US 2002036658 A1	28-03-2002
		US 2002013844 A1	31-01-2002
		US 2002016855 A1	07-02-2002
		US 2002023160 A1	21-02-2002
WO 0054477 A	14-09-2000	NL 1011524 C2	12-09-2000
		AU 2805800 A	28-09-2000
		WO 0054477 A1	14-09-2000
		EP 1159819 A1	05-12-2001
WO 0219585 A	07-03-2002	AU 7922501 A	13-03-2002
		AU 8321201 A	13-03-2002
		WO 0219595 A2	07-03-2002
		WO 0219585 A1	07-03-2002